שער דף השער יכלול את הפרטים הבאים: )כמובן שעיצוב / תמונות רקע וצבעים יתקבלו בברכה( 1 .לוגו בית הספר 2 .שם בית הספר 3 .שם העבודה 4 .שם התלמיד 5 .ת.ז. התלמיד 6 .שם המנחה 7 .שם החלופה 8 .תאריך ההגשה

Contents

[מבוא 4](#_Toc103165816)

[ייזום 4](#_Toc103165817)

[תיאור ראשוני של המערכת 4](#_Toc103165818)

[הגדרת הלקוח 4](#_Toc103165819)

[הגדרת יעדים 4](#_Toc103165820)

[בעיות תועלת וחסכונות 4](#_Toc103165821)

[סקירת פתרונות קיימים 4](#_Toc103165822)

[סקירת טכנולוגיות הפרויקט 4](#_Toc103165823)

[תיחום הפרויקט 6](#_Toc103165824)

[פירוט תיאור המערכת 6](#_Toc103165825)

[תיאור מפורט של המערכת 6](#_Toc103165826)

[תכנון וניהול לוח זמנים 6](#_Toc103165827)

[ניהול סיכונים והדרכים להתמודד איתם 7](#_Toc103165828)

[תיאור תחום הידע 7](#_Toc103165829)

[מסך הרשמה 7](#_Toc103165830)

[מסך כניסה 8](#_Toc103165831)

[מסך ניהול חסימות 8](#_Toc103165832)

[מסך מחיקת משתמש 9](#_Toc103165833)

[ארכיטקטורה של הפרויקט 9](#_Toc103165834)

[תיאור חומרה 9](#_Toc103165835)

[תיאור הטכנולוגיה הרלוונטית 10](#_Toc103165836)

[תיאור זרימת המידע 11](#_Toc103165837)

[דף הרשמה 11](#_Toc103165838)

[דף כניסה 12](#_Toc103165839)

[דף חסימת אתרים 13](#_Toc103165840)

[דף מחיקת משתמשים 14](#_Toc103165841)

[תיאור האלגוריתמים המרכזיים בפרויקט 15](#_Toc103165842)

[תיאור סביבת הפיתוח 15](#_Toc103165843)

[תיאור פרוטוקולי התקשורת 17](#_Toc103165844)

[UDP 17](#_Toc103165845)

[TCP 17](#_Toc103165846)

[SSL 19](#_Toc103165847)

[תיאור מסכי מערכת 20](#_Toc103165848)

[מסך הרשמה 20](#_Toc103165849)

[מסך כניסה 20](#_Toc103165850)

[מסך חסימת אתרים 21](#_Toc103165851)

[מסך מחיקת משתמש 22](#_Toc103165852)

[היררכיית דפים 23](#_Toc103165853)

[תיאור מבני הנתונים 23](#_Toc103165854)

[מסד הנתונים הראשי (SQLITE) 23](#_Toc103165855)

[קובץ HOST 23](#_Toc103165856)

[סקירת חולשות ואיומים 23](#_Toc103165857)

[פיצוח סיסמא 23](#_Toc103165858)

[SQL INJECTION 24](#_Toc103165859)

[DDOS 24](#_Toc103165860)

[ראיית המידע שעובר 24](#_Toc103165861)

[הזרקת קוד 24](#_Toc103165862)

[מימוש הפרויקט 24](#_Toc103165863)

[מודולים מיובאים 24](#_Toc103165864)

[re 24](#_Toc103165865)

[socket 24](#_Toc103165866)

[uuid 24](#_Toc103165867)

[typing 25](#_Toc103165868)

[ctypes 25](#_Toc103165869)

[sys 25](#_Toc103165870)

[netifaces 25](#_Toc103165871)

[openssl 25](#_Toc103165872)

[sqlite3 25](#_Toc103165873)

[tkinter 25](#_Toc103165874)

[logging 25](#_Toc103165875)

[SSL 25](#_Toc103165876)

# מבוא

## ייזום

### תיאור ראשוני של המערכת

הפרויקט נודע כדי לחסום אתרים על פי DOMAIN שלהם ולחסום את זה בכל האתרים בהם נמצאה המוצר באותו רשת, בחרתי בפרויקט הזה כי גיליתי על הקובץ HOST שמאפשר לך להגדיר באופן סטטי את הכתובת IP שלה DOMAIN. התאגרים שאני צופה לי בפרויקט הם שיהיה לי קשה לסכרן שכל המחשבים יחסמו את אותם אתרים כל הזמן, ושמירה על המידע המעובר כדי למנוע לפגוע במידע שעובר ובמידע שנשמר במחשב.

### הגדרת הלקוח

המערכת מיודעת להורים שרוצים להגן על ילדיהם מפני אתרים עם תכנים שלא מתאימים להם בנוסף הוא מאפשר לתת עונש ליליד באמצעות חסימת אתרים שבהם הוא משחק.

### הגדרת יעדים

המטרות המרכזיות בפרויקט היא לחסום אתרים על פי רצונו של ההורה, בנוסף המטרות המשניות בפרויקט זה לסכרן את כל המחשבים שמחוברים כך שכולם יחסמו את אותם אתרים, ליצור ממשק משתמש נוח ולהגן על פרטי משתמש.

### בעיות תועלת וחסכונות

הבעיה המרכזית שהמערכת מנסה לפתור היא שהורים אינם יכולים לפקח איפה ילדיהם גולשים באינטרנט וכדי למנוע מצבים שבהם ילדיהם נמצאים באתר שהם לא היו רוצים שהם יהיו בו. המערכת תספק את היכולת למנוע את הגישה לאותם אתרים.

### סקירת פתרונות קיימים

פתרונות אחרים קיימים בכמה צורות כאשר העיקרית היא לנתר את ולחסום את האתרים ישירות דרך הנתב כמו לדוגמה סינון תכנים של בזק. קיימים עוד סוגים שבהם ניתן לחסום כגון חסימה באמצעות שינוי חוקי FIREWALL ועוד.

### סקירת טכנולוגיות הפרויקט

בכדי למנוע גישה לאותם אתרים אני מסתמך על קובץ HOST שקיים רק במערכת ההפעלה WINDOWS וכי על מנת שהקוד יעבוד כמו שצריך חובה להריץ אותו רק על WINDOWS, בנוסף לכך על מנת לקבל גישה לקובץ על המשתמש לאשר קבלת גישת מנהל למחשב.

### תיחום הפרויקט

התחומים בהם הפרויקט עוסק הינם: רשתות כאשר בעיקר יש דגש על הפרוטוקולים הבאים: TCP, UDP ו DNS. הפרויקט מתעסק מעט במערכות הפעלה כאשר צריך לקבל גישה על מנת לנהל את הקובץ HOST וקבלת גישות מנהל.

## פירוט תיאור המערכת

### תיאור מפורט של המערכת

המערכת חוסמת אתרים באמצעות קובץ HOST הנמצא בכל מחשב שעליו קיימת מערכת ההפעלה WINDOWS. המערכת בכל מחשב מתקשרת אם שאר המערכות בחשבים אחרים על מנת לגרום לכך שכולם יחסמו את אותם אתרים. כאשר מתקינים את המערכת בפעם הראשונה צריך להכניס שם משתמש וסיסמא על מנת שרק הבן אדם שהתקין את המערכת יוכל לשנות אילו אתרים המערכת חוסמת. ובכדי לעשות זאת המערכת מנהל בסיס נתונים יחסי שמאפשר שמירת מידע לאורך זמן. הסיסמאות מאובטחות באמצעות פונקציית SHA-256. המערכת מציגה את האופציות השונות שקיימות למשתמש באמצעות ממשק גרפי ייחודי.

### תכנון וניהול לוח זמנים

היעדים להם צריך להיות מוענים עם הפרויקט היו:

8/5 תאריך הגשת ספר פרויקט.

20/5 תאריך הגשת הפרויקט.

כאשר התחלתי לעבוד על הפרויקט התלתי בכך שפתחתי קובץ טקסט והתחלתי לרושם איך הייתי רוצה שהפרוייקט יראה אחר כך רשמתי מה עלי ללמוד על מנת לבצע את הפרויקט. ברגע שהבנתי מה עלי ללמוד התחלתי ללמוד ולהתנסות באותם נושאים כאשר ייצרתי כל מיניי מיני-פרוייקטים שמבוססים רק על אותם ספריות שעלי ללמוד. אחר כך תכננתי לוח זמנים כאשר התחלתי לעבוד על הקוד של הפרויקט בתחילת חופשת פסח.

על מנת לתכנן לוח זמנים נכון חילקתי את הפרויקט לשני חלקים הראשון הקוד והשני הספר כאשר את הקוד חילקתי לעוד כמה חלקים.

הינה הלוח זמנים:

תקשורת בין המחשבים – 15/4-18/4

הצפנת התקשורת -19/4

ניהול מסד הנתונים – 20/4-22/4

ניהול קובץ ה HOST – 23/4

יצירת ממשק משתמש בסיסי – 24/4-28/4

חיבור כל החלקים יחד – 29/4-30/4

תיקון באגים -31/4-1/5

כתיבת ספר פרויקט- 2/5 – 8/5

אם צריך לשפר את נראות ממשק המשתמש ותיקון באגים שצצים – 9/5-20/5

### ניהול סיכונים והדרכים להתמודד איתם

הסיכונים העיקריים בפרויקט הם בשמירת שמות משתמשים וסיסמאות ועל מנת להתמודד בסיכון של לקיחת הסיסמאות ובכך להצליח לשנות את האתרים הנחסמים על מנת להתמודד עם זה אני מצפין את הסיסמא באמצעות SHA-256 ובכך גורם לאופציה שדרך מסד הנתונים יגלו את הסיסמא לבלתי אפשרית.

עוד סיכון קיים בשינוי המידע העובר על מנת להתמודד עם זה כל המידע העובר הנוגע למסד הנתונים מוצפן באמצעות פרוטוקול SSL.

## תיאור תחום הידע

### מסך הרשמה

מהות: רישום משתמש חדש במערכת

אוסף יכולות נדרשות:

ממשק משתמש – מסך הרשמה

קליטת נתונים

בדיקת תיקנות של אותם נתונים האם המשתמש קיים והאם הסיסמא מתאימה למגבלות ואם לא הצגת תגובה מתאימה

הצפנת הסיסמא

שליחת הנתונים לכל שאר המחשבים בצורה מאובטחת.

הצגת מסך הכניסה למשתמש

אובייקטים נחוצים: ממשק משתמש, הצפנה, תקשורת, בסיס נתונים

### מסך כניסה

מהות: כניסת משתמש

אוסף יכולות נדרשות:

ממשק משתמש – מסך כניסה

קליטת נתונים

הצפנת הסיסמא

בדיקה במסד הנתונים האם השם משתמש והסיסמא תואמים ואם הם לא הצגת תגובה מתאימה

ממשק משתמש - הצגת מסך ניהול החסימות

אובייקטים נחוצים: ממשק משתמש, הצפנה, בסיס נתונים

### מסך ניהול חסימות

מהות: ניהול חסימת האתרים

אוסף יכולות נדרשות:

ממשק משתמש – הצגת מסך ניהול חסימות

קליטת הDOMAIN מהמשתמש

מחיקת DOMIAN

הוספת DOMAIN

אם נוסף או נמחק DOMAIN לעדכן את שאר המחשבים על כך.

סכרון מסד הנתונים של שאר המחשבים

ממשק משתמש – הצגת מסך מחיקת משתמש

אובייקטים נחוצים: ממשק משתמש, הצפנה, תקשורת, בסיס נתונים, קובץ HOST.

### מסך מחיקת משתמש

מהות : מחיקת משתמש

אוסף יכולות נדרשות:

ממשק משתמש -הצגת מסך מחיקת משתמש

קליטת סיסמא מהמשתמש

הצפנת הסיסמא מהמשתמש

בדיקת הסיסמא במסד הנתונים

מחיקת המשתמש

עדכון שאר המחשבים על כך שמשתמש נמחק

ממשק משתמש העברה למסך הרשמה או כניסה בהתאם למסד הנתונים

אובייקטים נחוצים: ממשק משתמש, הצפנה, תקשורת, בסיס נתונים

# ארכיטקטורה של הפרויקט

## תיאור חומרה

הרשת מורכבת מנתב שעליו מחוברים כל המחשבים כאשר כל מחשב מספק כשרת וכלקוח בו זמנית כאשר המידע עובר דרך הנתב אל כל שאר המחשבים.

Diagram

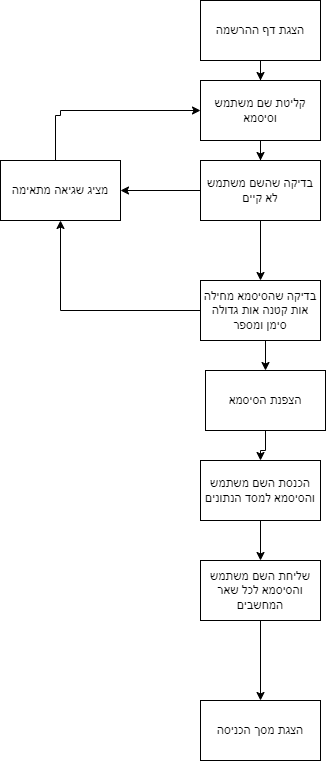
Description automatically generated

## תיאור הטכנולוגיה הרלוונטית

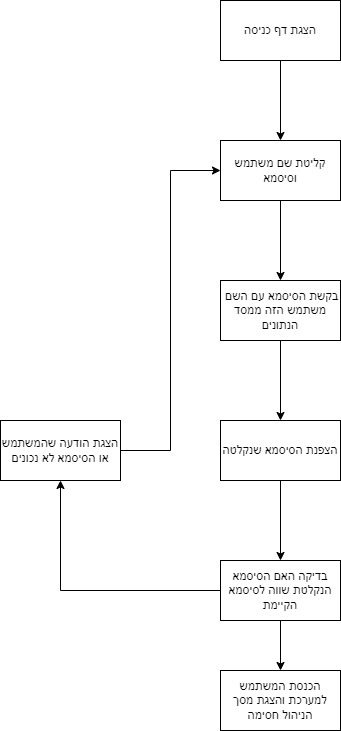
בפרויקט אני משתמש בשתי שפות תכנות: פייתון ו SQL, ובמערכת ההפעלה WINDOWS, כאשר הפרוטוקולים שבהם אני משתמש הם TCP,UDP,SSL,DNS ו HTTP.

## תיאור זרימת המידע

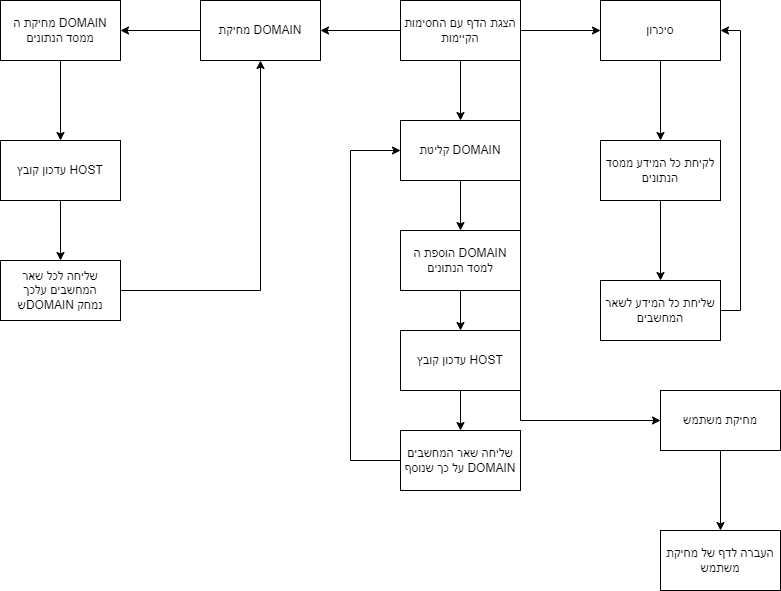
### דף הרשמה



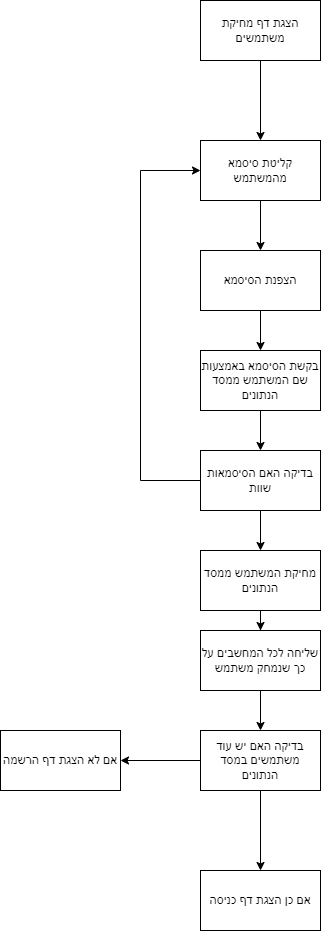
### דף כניסה



### דף חסימת אתרים



### דף מחיקת משתמשים



## תיאור האלגוריתמים המרכזיים בפרויקט

#### מיון כתובות IP:

כדי לדעת את ה IP של המחשב אני מקבל רשימה של מילונים שבהם נמצאים ה IP של המחשב הSUBNET-MASK וכתובת ה BROADCAST של הSUBNET אבל כדי לדעת מה ה IP האמיתי של הפרויקט גיליתי שזה תמיד ה IP השני בסדר ולכן עלי למיין את הרשימה על פי סדר ה IP.

על מנת למיין את הרשימה יש לעבור על כל IP ולבדוק האם הוא הקטן ביותר עושים זאת באמצעות לחלק את ה IP לארבע חלקים כאשר מפצלים אותם לפי הנקודה ואז ממיינים אותם לפי ששל מי החלק השמאלי קטן יותר הוא קטן יותר מהאחד שמשווים מולו ואם הם שווים עוברים לחלק הבא וכך הלאה.

הסיבה שעשיתי את אלגוריתם מיון זה הוא כי רציתי משהו פשוט שייתן לי את ה IP הנכון אופציות אחריות היו למיין את הIP על פי אלגוריתם מיון מהר יותר אך בסדר גודל של הIP שבהם יש במחשב ההבדל הוא בכמה אלפיות השנייה ולכן זה לא מאוד משנה.

#### להתמודד עם תשובות BROADCAST

על מנת להוסיף את המחשבים שאליהם מותקנת האפליקציה כל מחשב שולח כל 5 שניות פקטת BROADCAST של UDP שבה נשלח “who is up” וכל שאר המחשבים שקולטים זאת שולחים לאותו מחשב תשובה עם השם של המחשב כתובת ה IP ה SUBNET MASK, PORT, ו כתובת MAC. תוך כדי במחלקה הנקראת MultiSocket יש מילון שמכיל את הIP של המחשב ששלח את ההודעה שביקשה את המידע הנ"ל כמפתח והערך היינו האובייקט של המחשב. כאשר האובייקט של המחשב כרגע מכיל רק את הIP שלו.

כאשר המחשב ששלח את ה BORADCAST הראשון רואה את ה BROADCAST השני הוא מוסיף את האובייקט של המחשב שלו למילון שלו ופותח ערוץ תקשורת עם המחשב השני.

על מנת שלמחשב השני יהיה את ערוץ התקשורת של הסרבר של המחשב השני קורה אותו תהליך רק ששני המחשבים מתחלפים בתפקיד.

#### להתמודד עם הודעות של קליינטים

על מנת לסכרן את מסד הנתונים בין כל המחשבים אני שולח בקשות לשאר המחשבים דרך ה ערוצי תקשורת שפתוחים איתם ואני שולח שלושה סוגי הודעות הוספת משתמש, מחיקת משתמש, הוספת כתובת, מחיקת כתובת. על מנת למנוע זיוף של הודעות וקריאת פרטים אישיים כל הערוצי תקשורת מוצפנים באמצעות SSL כאשר בכל פועלה כאשר ערוץ התקשורת מזהה את אחת מסוגי ההודעות הללו הוא גם משנה את מסד הנתונים.

#### הרשמות לאפליקציה

על מנת להירשם לאפליקציה יש להביא שם משתמש וסיסמא כאשר השם משתמש לא יוכל להיות בשימוש כבר וכאשר הסיסמא צריכה להיות עם לפחות עם אות גדולה אות קטנה מספר וסמל כאשר כל הסיסמא חייבת להיות בגודל של מינימום 8 תווים.

## תיאור סביבת הפיתוח

הכלים הדרושים על מנת לפתח את האפליקציה הם פייטון, וSQL כאשר הסביבות בהם אני השתמשתי הם visual studio code ו pycharm.

## תיאור פרוטוקולי התקשורת

### UDP

UDP הינו פרוטוקול תקשורת הנמצא בשכבה הרביעית כאשר הוא מאפשר מעבר נתונים דרך כתובות IP ושיוכם לאפליקציות דרך פורט שמשויך לאפליקציה. פרוטוקול זה מספק העבר נתונים מהירה אך לא אמינה כאשר אפשר להשתמש בו גם להעברת בקשות BROADCAST כאשר כתובת היעד בהם היא לא של מחשב ספציפי אלה של כל המחשבים וכל המחשבים יכולים לראות זאת.

למרות שפרוטוקול זה אינו אמין הוא מספק בדיקה מסוימת במסגרת מספר מיוחד הנקרא checksum כאשר פונקציית ה-Checksum מבצעת את החישוב הבא: חילוק ההודעה לקטעים של 16 סיביות, סכימת כל הקטעים והוספת השארית. לאחר מכן התוצאה נשללת לפי ייצוג One's Complement - כל ביט 0 מוחלף ב-1 ולהפך.

חלוקת הבתים בפרוטוקול זה היא לפי הדברים הבאים:

פורט המקור (16 סיביות) - שדה המכיל את מספר הפורט במחשב המקור. שדה אופציונלי, מאחר שפרוטוקול UDP לא מקיים בהכרח תקשורת דו כיוונית. במקרה ואינו בשימוש השדה יכיל אפסים.

פורט היעד (16 סיביות) - שדה המכיל את מספר הפורט במחשב היעד.

אורך החבילה (16 סיביות) - שדה המכיל את אורך פתיח הUDP והמידע ביחידות של בתים. יש להבדיל משדה "אורך החבילה" שבפתיח של חבילת IPv4 שמכיל את אורך החבילה כולה, בעוד ש"אורך החבילה" בפתיח הUDP לא מכיל את פתיח פקטת הIPv4, שגודלו נע בין 20 ל60 בתים.

סיכום ביקורת (16 סיביות) - checksum, מספר האימות של הפתיח והנתונים. שדה אופציונלי, שבמידה ולא ימומש יכיל רשומה מלאה ב-0 בינארי.

סוגי ההודעות שנשלחות דרך פרוטוקול זה הם:

1. “who is up” – על מנת לדעת אילו מחשבים האפליקציה רצה אליהם כאשר התשובה שמקבים מהמחשבים האחרים היא על פי הפורמט הבא.
2. “ip, subnet mask, mac, port, computer name, up” בעצם ככה נשלח כל המידע הרלוונטי על המחשב הזה. וככה הוא נשלח לכל המחשבים והם יכולים להוסיף אותם ככה.

### TCP

TCP הינו פרוטוקול תקשורת הנמצא בשכבה הרביעית כאשר הוא מאפשר מעבר נתונים דרך כתובות IP ושיוכם לאפליקציות דרך פורט שמשויך לאפליקציה. אך כאשר פותחים ערוץ תקשורת TCP עם מחשב מסוים נוצר תהליך לחיצת יד משולשת כאשר המחשב שיוזם את פתיחת התקשורת שולח למחשב בקשת SYN שמטרת להגיד למחשב השני שאני רוצה לסכרן איתו את החיבור, המחשב השני עונה SYN ACK כאשר זה אומר שהמחשב השני קיבל את ההודעה ומסוכרן איתך והמחשב הראשון שולח בסוף ACK כדי לסיים את לחיצת היד ולהבהיר למחשב שהכל הגיע. מכאן כל פעם שמידע עובר על מנת לוודא שהוא הגיע כמו שצריך המחשב שמקבל את ההודעה שולח ACK למחשב ששלח את ההודעה.

בנוסף לכך כדי להבטיח שהמידע עובר כמו שצריך אם לא מתקבלת תושבת ACK הפקטה נשלחת שוב עד שיש TIMOUT שנקבע מראש על פי מערכת ההפעלה או על פי מי שפתח את ערוץ התקשורת.

עוד אמצעים לוודא שהמידע עובר כמו שצריך הם:

* מספור הפקטות כאשר מפצלים אותם כדי לוודא שהמידע מחובר בחזרה בצורה הנכונה.
* Checksum כמו ב UDP.

חלוקת הבתים בפרוטוקול זה הוא בצורה הבאה:

פורט המקור (16 סיביות) - שדה המכיל את מספר הפורט במחשב המקור.

פורט היעד (16 סיביות) - שדה המכיל את מספר הפורט במחשב היעד.

מספר סידורי (32 סיביות) - נבחין בין שני מקרים:

דגל SYN נושא ערך "1" (החבילה היא חלק מהקמת הקשר) - המספר בשדה מכיל את מספר החבילה שממנו יתחילו למנות (המספר הסידורי של חבילת המידע הראשונה יהיה למעשה המספר הזה + 1).

דגל SYN נושא ערך "0" (החבילה היא חלק מרצף התקשורת בין המחשבים) - המספר בשדה מכיל את מספר החבילה הנוכחית ביחס לתקשורת הפתוחה בין שני המחשבים (TCP session).

מספר אישור (32 סיביות) - (ACK) שדה מכיל את המספר הסידורי של ההודעה הבאה לה מצפה התחנה ומהווה אישור קבלה על כל ההודעות בעלות מספר סידורי הקטן ממנו. המידע בשדה תקף רק כאשר דגל ACK נושא ערך "1".

היסט המידע / אורך הפתיח (4 סיביות) - שדה זה מכיל את גודל הפתיח (ביחידות של 32 סיביות) של החבילה הנוכחית שהוא גם ההיסט מתחילת החבילה עד לתחילת המידע.

שמור (3 סיביות) - שדה השמור לשימוש עתידי (אמור להכיל אפסים).

דגלים (9 סיביות(

גודל חלון הקליטה (16 סיביות) - מספר הבתים אותם יכול המחשב לקלוט החל ממספר ההודעה שצוין בשדה מספר האישור (ACK).

סיכום ביקורת (16 סיביות) - checksum, מספר האימות של הפתיח וחלק מהפתיח של שכבת ה IP.

היסט למידע דחוף (16 סיביות) - אם דגל URG נושא ערך "1", הערך בשדה זה מציין את ההיסט למיקום מידע דחוף (לרוב אינו בשימוש).

אפשרויות שונות (0–40 בתים) - שדה אופציונלי שיכול להכיל בין היתר את גודל הסגמנט המרבי (Maximum Segment Size, MSS) לשימוש בפרוטוקול. גודל השדה נקבע על פי שדה "אורך הפתיח", אם האורך המצוין אינו גדול מ-5 שדה זה כלל לא נמצא.

ריפוד אפסים (0–4 בתים) - שדה שתפקידו למלא את הפתיח ב-"0" על מנת להגיע לכפולה שלמה של 32 סיביות.

ההודעות שנשלחות דרך פרוטוקול זה הם:

“still alive?” – לוודא שערוץ התקשורת עדיין פתוח ואין בעיה אתו.

"add domain {domain}" – להוסיף את הכתובת הנתונה למסד הנתונים

"remove domain {domain}" – למחוק את הכתובת הנתונה ממסד הנתונים

"add user {username} {encrypted password}" – להוסיף משתמש למסד הנתונים

"remove user {username}" - למחוק משתמש ממסד הנתונים

### SSL

SSL/TLS הוא פרוטוקול ורסטילי שמטרתו אבטחת שיחת שרת/לקוח בשיטות קריפטוגרפיות חזקות והוא אמור למנוע ציתות, זיוף, או חבלה (שינוי זדוני) של המידע העובר בין השרת והלקוח. מאפשר חיבור אנונימי, אימות שרת (חד-צדדי) או אימות דו-צדדי, תוך שמירה על דיסקרטיות ושלמות המסרים. שלוש נקודות עיקריות שהפרוטוקול אמור לתת להן מענה הן:

* **פרטיות** - המושגת באמצעות הצפנה סימטרית.
* **אימות** - המושג באמצעות תעודת מפתח ציבורי.
* **אותנטיות** - המושגת באמצעות קוד אימות מסרים.

אני משתמש בפרוטוקול זה רק כדי להצפין את המידע העובר דרך פרוטוקול TCP כדי שלא יהיה ניתן לראות אותו או לשכפל אותו ובכך לזייף בקשות.

## תיאור מסכי מערכת

### מסך הרשמה

#### תפקיד המסך

תפקיד המסך הזה הוא שהמשתמש יוכל להירשם למערכת באמצעות הכנסת שם משתמש וסיסמא.

#### תיאור המסך

המסך מציג מקום בו ניתן להכניס שם משתמש ועוד מקום בו ניתן להכניס סיסמא כאשר בנוסך לכך יש כפתור שאפשר להירשם איתו כאשר לוחצים עליו הקוד בודק האם השם משתמש קיים במערכת והאם הסיסמא עונה על מספר קריטריונים. כאשר נוסף משתמש נשלח המידע על כך שנוסף משתמש לכל המחשבים. נוסף על כך יש כפתור שיוצר את המסך מחדש כך שאם נוצר משתמש בדיוק במחשב אחר אפשר ללחוץ על הכפתור והוא יעביר אותך לדף חסימת האתרים.

A picture containing graphical user interface

Description automatically generated

### מסך כניסה

#### תפקיד המסך

תפקיד המסך הוא שהמשתמש יוכל להיכנס למערכת באמצעות השם משתמש והסיסמא שנכנס איתם לפני.

#### תיאור המסך

במסך יש מקום לשים שם משתמש וסיסמא כאשר יש כפתור להיכנס שהוא בודק האם המשתמש קיים ואם כן האם הסיסמא מתאימה למשתמש הזה אם כן הוא מעביר אותו לדף חסימת המשתמשים, בנוסף קיים כפתור היוצר את הדף מחדש כך שאם נמחק המשתמש הוא יעביר את המשתמש לדף ההרשמה.

Text

Description automatically generated with medium confidence

### מסך חסימת אתרים

#### תפקיד המסך

להציג, להוסיף ולמחוק אתרים שחסומים.

#### תיאור המסך

במסך מוצגים כל האתרים החסומים כאשר ליד כל אחד יש כפתור למחוק את האתר כאשר לוחצים על הכפתור הוא מוחק אותו ממסד הנתונים, מוחק אותו מקובץ HOST, ושולח לכל המחשבים על כך שנמחק DOMAIN. בנוסף לכך יש מקום לרשום DOMAIN כאשר לוחצים עליו הוא מוסיף את ה DOMAIN למסד הנתונים, מעדכן את קובץ HOST ו מעדכן כל המחשבים על כך שנוסף DOMAIN. יתר על כן ישנו כפתור של סכרון הנתונים שתפקידו לשלוח את כל המידע של מסד הנתונים לכל שאר המחשבים ובכך לסכרן את מסד הנתונים שלו עם של כולם. זאת ועוד קיים כפתור המעביר אותך לדף של מחיקת משתמש. וגם קיים כפתור היוצר את הדף מחדש ובכך אם היה שינוי במסד הנתונים בגלל שינוי שקרא במסך אחר הוא יופיע גם במסך הזה.

Graphical user interface, application

Description automatically generated

### מסך מחיקת משתמש

#### תפקיד המסך

למחוק משתמש קיים

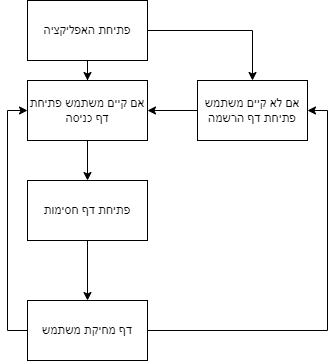
#### תיאור המסך

במסך יש מקום לשים את הסיסמא וכפתור למחיקת הסיסמא כאשר לוחצים עליו הוא לוקח את הסיסמא על פי המשתמש ובודק האם הסיסמא המוצפנת שהוכנסה שווה לסיסמא ממסד הנתונים אם כן הוא מוחק את המשתמש ומעדכן את שאר המחשבים על כך אחר כך הוא פותח או את דף ההרשמה או את דף הכניסה דבר זה תלוי בהאם יש עוד משתמשים.

Graphical user interface

Description automatically generated with medium confidence

## היררכיית דפים



## תיאור מבני הנתונים

### מסד הנתונים הראשי (SQLITE)

מסד נתונים זה מכיל שתי טבלאות הראשונה שייכת לאכסון פרטי המשתמש כאשר שם כלול שם המשתמש כ TEXT מה שאומר שהוא מכיל טקסט שגודלו בלתי מוגבל, וכלול שם גם הסיסמא גם כן כ TEXT.

הטבלה השנייה במסד הנתונים הזה היא הטבלה שמכילה את האתרים הנחסמים כך שבטלה זו נכלל רק שדה אחד שהוא ה DOMAIN של האתר שרוצים לחסום

### קובץ HOST

בקובץ זה נכללים הDOMAIN של האתרים ולאיזה IP הDOMAIN הזה מוביל כך שאם מסתכלים עליו הוא נראה כך:

127.0.0.1 google.com

## סקירת חולשות ואיומים

### פיצוח סיסמא

האיומים היכולים לקרות על המערכת הם בעיקר ניסיון פיצוח סיסמא מכיוון שלא קיים מנגנון שמנוע ממך לנסות כמה סיסמאות שאתה רוצה אך כדי להתמודד עם כך הסיסמא חייבת להיות בעלת 8 תווים כאשר לפחות אחד מהם עם אות גדולה, אות קטנה, מספר וסימן ולכן כמות האפשרויות מאוד גדולה ולכן קשה מאוד לפרוץ לסיסמא בטח עם BRUTEFORCE. ובגלל שגם כל הסיסמאות מוצפנות באמצעות SHA-256 לכן לא ניתן לדעת את הסיסמא מבלי לנסות מלא פעמים.

### SQL INJECTION

יכול להיות שקיימים חולשות במסד הנתונים בגלל שאינני בודק האם קלט שמגיע מהמשתמש הוא שאילתת SQL אך אני לא מציג למשתמש נתונים ממסד הנתונים אלה אני רק מאכסן אותם ובודק אותם ואי אפשר להיכנס באמצעות הזרקת קוד SQL לקלט.

### DDOS

למערכת אכן ניתן לעשות DDOS אך לעשות דבר זה יכול להרוג את הנתב לפני שזה יהרוג את המערכת ולכן דבר זה בלתי סביר בעליל.

### ראיית המידע שעובר

כל המידע האישי שעובר, עובר דרך ערוצי תקשורת על TCP שהם מוצפנים באמצעות SSL מה שאומר שלא יהיה ניתן לראות את המידע שעובר אלה אם כן יש בדידי הפורץ גישה לCERTIFICATE של המחשבים.

### הזרקת קוד

הזרקת קוד לא אפשרית בגלל שכל הקוד נמצא קובץ EXE או כPYI שהם בלתי קריאים וקשה מאוד לשנות אותם כדי שיתנו את הפלט הרצוי.

# מימוש הפרויקט

## מודולים מיובאים

### re

מודול זה מאפשר שימשו בביטויים רגולריים בפיתון ובדיקת קלט מסוים כלפיהם. המודול מיועד על מנת לבדוק האם הסיסמא מכילה 8 תווים שכוללים לפחות אות גדולה, אות קטנה, מספר וסימן.

### socket

מודול האחראי לפתיחת ערוצי התקשורת והעברת המידע דרכם, משומש בכל ערוצי התקשורת גם TCP וגם UDP.

### uuid

ספרייה המתעסקת בהבאת מזהים יחודיים, משומשת על מנת להשיג את כתובת ה MAC של המחשב.

### typing

ספרייה המשתמש לנתינת רמזים על הטיפוסים של כל משתמש ואיזה טיפוס הפונקציה מחזירה. משומש בכמעט כל פונקציה בפרויקט וכמעט כל משתנה בפרויקט.

### ctypes

ספרייה המאפשרת קריאה וביצועם של קבצי DLL. ספרייה זו משתמשת על מנת להריץ את הקוד כמנהל מערכת.

### sys

ספרייה זו מספקת פונקציות ומשתנים שונים המשמשים לתמרן חלקים שונים של סביבת הריצה של פיתון. ספרייה זו משתמש גם כן על מנת להריץ את הקוד כמנהל מערכת.

### netifaces

ספרייה המשתמש על מנת לספק ספירת ממשקי רשת ופירוטם במחשב. משומש בפרויקט על מנת לראות את כל כתובת ה IP של המחשב ובחירת הIP הנכון.

### openssl

ספרייה המשתמש ליצירת certificates באופן פשוט באמצעות כל מיני משתנים.

### sqlite3

ספרייה המשתמש ליצירה ועריכתה של מסד הנתונים כך שהוא שיכלול את הנתונים הרצויים. משומש בכל הפרויקט על מנת ליצור ולערוך את מסד הנתונים.

### tkinter

ספרייה המשמשת על מנת ליצור ממשק משתמש פשוט ונוח.

### logging

ספריה המשמשת לרישום נוח על מנת ליצור הודעות בקרה למערכת.

### SSL

ספריה המשמשת על מנת להפוך את ערוצי התקשורת למוצפנים באמצעות פרוטוקול SSL.

## מחלקות ומודלים כתובים

### Computer

מחלקה זאת נועדה על מנת לייצג מחשב במערכת של המחלקה הם (*המשתנים הרשומים כך הינם property*):

*ip* - כתובת הIP של המחשב הזה.

*name* - השם של המחשב.

*mac*- כתובת ה MAC של המחשב.

*port* – הפורט שדרכו מתחברים לשרת של המחשב הזה.

server\_socket – ערוץ התקשורת שפתוח בין השרת שנמצא על המחשב שמיוצג על ידי המחלקה לבין המחשב שאליו רץ הקוד.

client\_socket – ערות התקשורת שפתוח בין השרת שעליו רץ הקוד לבין המחשב שמיוצג על ידי המחלקה.